WHAT IS CLAIMED IS

1. A cryptographic device which encrypts input data by sequentially processing it by a plurality of round processing which nonlinearly transforms it using extended key, comprising:

an initial splitting part which splits the input data to two pieces of block data;

a key storage part for storing extended key;

a plurality of cascade-connected round processing parts which are supplied with said two pieces of block data and sequentially process them using said extended key; and

a final combining part which combines two pieces of block data output from the last round of said plurality of cascade-connected round processing parts into a single piece of data and outputs it;

wherein each of said plurality of round processing part comprises:

a nonlinear function part which transforms one of two pieces of block data input thereto from the preceding stage, depending on extended key stored in said key storage part;

a linear operation part which linearly operates the output data from said nonlinear function part and the other of said two pieces of block data; and

a swapping part which swaps the output data from said linear operation part and the input block data to said nonlinear function part and provides the two pieces of swapped data as two pieces of input block data to said round processing part of the next round; and

wherein said nonlinear function part comprises:

a key-dependent linear transformation part which linearly transforms input data based on extended key stored in said key storage part to thereby generate transformed data;

a splitting part which splits the transformed data from said key-dependent linear transformation part to a plurality of bit strings;

a plurality of first nonlinear transformation parts which nonlinearly transform these bit strings, respectively, and output transformed data;

a first linear transformation part which linearly transforms the transformed data from said plurality of first nonlinear transformation parts in association with each other and outputs a plurality of pieces of uniformed data to a plurality of routes, respectively;

a second nonlinear transformation part provided in at least one of said plurality of routes, for nonlinearly transforming said uniformed data from the corresponding one of said first linear transformation parts, and for outputting the transformed data as data of that route; and

a final combining part which combines data from said plurality of routes into output data of said nonlinear function part.

2. The cryptographic device of claim 1, wherein said first linear transformation part comprises a key-dependent linear operation part which linearly transforms said plurality of pieces of uniformed data based on extended key stored in said key storage part and outputs the plurality of transformed data as data of said plurality of routes.

3. The cryptographic device of claim 1 or 2, wherein there is provided a second linear transformation part which linearly transforms the output data from said combining part to provide the output data of said nonlinear function part.

4. The cryptographic device of claim 3, wherein said second linear transformation part is a linear transformation part which performs a linear transformation based on extended key stored in said key storage part.

5. The cryptographic device of claim 4, wherein said first linear transformation part comprises at least one exclusive OR circuit provided in each of said plurality of routes, for outputting said uniformed data to said each route by an exclusive-OR operation of data of said each route and data of other routes.

6. The cryptographic device of any one of claims 1 through 5, wherein there is provided an initial linear transformation part which linearly transforms said input data and supplies it to said initial splitting part.

7. The cryptographic device of claim 6, wherein said initial linear transformation part is a transformation part which performs a linear transformation based on extended key stored in said key storage part.

8. The cryptographic device of any one of claims 1 through 7, wherein there is provided a final linear transformation part which linearly transforms the output data of said final combining part to provide it as the output of said cryptographic device.

9. The cryptographic device of claim 8, wherein said final linear transformation part is a transformation part which performs a linear

transformation based on extended key stored in said key storage part.

10. The cryptographic device of any one of claims 1 through 9, wherein said plurality of routes are first, second, third and fourth routes arranged in this order.

11. The cryptographic device of claim 10, wherein said second nonlinear transformation part is provided in each of said four routes.

12. The cryptographic device of claim 10, wherein said second nonlinear transformation part is provided in each of said first and fourth routes.

13. The cryptographic device of claim 12, wherein said first linear transformation part comprises:

a first exclusive OR circuit provided in said second route, for carrying out the exclusive-OR between data of said first route and data of said second route;

a second exclusive-OR circuit provided in said third route, for carrying out the exclusive OR between data of said fourth route and data of said third route;

a third exclusive-OR circuit provided in said third route, for carrying out the exclusive OR between the output of said second exclusive-OR circuit and the output of said first exclusive-OR circuit;

a fourth exclusive-OR circuit provided in said second route, for carrying out the exclusive OR between the output of said first exclusive-OR circuit and the output of said third exclusive-OR circuit;

a fifth exclusive-OR circuit provided in said first route, for carrying out the exclusive OR between the data of said first route and the output of said fourth exclusive-OR circuit; and

a sixth exclusive-OR circuit provided in said fourth route, for carrying out the exclusive OR between the data of said fourth route and the output of said third exclusive-OR circuit.